L21: Entry 2 of 13 File: PGPB Jun 3, 2004

PGPUB-DOCUMENT-NUMBER: 20040107027
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20040107027 A1

TITLE: Safety Aircraft Flight System

PUBLICATION-DATE: June 3, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY
Boudrieau, Gary Jon	North Lakewood	WA	US

APPL-NO: 10/605625 [PALM]
DATE FILED: October 14, 2003

RELATED-US-APPL-DATA:
child 10605625 A1 20031014
parent continuation-of 60319613 20021011 US PENDING

INT-CL: [07] G05 D 1/00

US-CL-PUBLISHED: 701/001; 340/574
US-CL-CURRENT: 701/1; 340/574

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

The present invention is a computer system designed to use the conventional devices and special programming of the present invention that will ensure the safe operation of aircraft. The present invention is an anti-terrorist and anti-crash system to ensure and maintain complete control of an aircraft on the ground, during taxiing and even in the air. With the present invention in place, an aircraft can be kept a safe distance from any building and other aircraft, and the aircraft can be remotely controlled. The system provides greater national security. Utilizing the on-demand audio and visual monitoring components of the present invention, simultaneously, proper authorities can access all factual data from all onboard flight systems before a crash is imminent. Equipment lockouts are in place as well, so that if an aircraft is commandeered, the actual person in the cockpit is unable to effect aircraft travel, virtually eliminating human error.

L21: Entry 1 of 13 File: PGPB Dec 2, 2004

DOCUMENT-IDENTIFIER: US 20040239550 A1
TITLE: Weather incident prediction

Application Filing Date:
20040413

Summary of Invention Paragraph:
[0031] One U.S. Pat. No. 5,739,770, entitled Off-Path Descent Guidance By A Flight Management System, issued to Liden on Apr. 14, 1998, the complete disclosure of which is incorporated herein by reference, discloses a method for providing off-path guidance during a descent. Another U.S. Pat. No. 4,811,230, entitled Intervention Flight Management System, issued to Graham, et al on Mar. 7, 1989, the complete disclosure of which is incorporated herein by reference, discloses an Intervention Flight Management System (IFMS) that allows a pilot to intervene in the operation of a preprogrammed flight management computer and change the speed and/or flight path of an aircraft in response to air traffic control (ATC) instructions using lateral and vertical control subroutines that override the preprogrammed instructions controlling the flight management computer, thereby reducing pilot workload when pilot attention should be focused on flight progress.

Summary of Invention Paragraph:
[0036] One of the many functions of a FMS is to use a simulation algorithm to construct a sequence of waypoints and connecting line segments that is referred to as a "flight plan" shown in FIGS. 6A and 6B. FIG. 6A illustrates a horizontal view 40 of the flight plan. In operation, the pilot, after takeoff, selects the route to be flown and establishes a flight plan, which the pilot then inputs into the FMS via the CDU. The FMS constructs a flight path 42 from the aircraft position to the destination, which is then used as a reference for lateral and vertical guidance. The lateral component of the path is defined by waypoints 44 and various types of line segments 46 connecting the waypoints 44. The flight plan begins at the origin runway threshold (not shown) and ends at the end of descent point E/D. 14. The FMS is coupled to the aircraft's autothrottle (not shown) and autopilot (not shown) for effecting airspeed changes.

Summary of Invention Paragraph:
[0037] FIG. 6B illustrates the vertical component 48 of the flight plan, which is composed of three principal phases of flight: climb, cruise and descent. As part of the performance function of a FMS, a descent path is constructed from a T/D (top of descent) point at the final cruise altitude, to a defined E/D (end of descent) point with a prescribed altitude constraint. The E/D point may, for example, be the destination runway threshold, 50 feet above the runway, or it may be some other earlier waypoint, such as the FAF (final approach fix). The E/D point is selected as part of the flight planning function of the FMS. The descent path is then constructed so that the aircraft will arrive at the E/D point using selected speed and thrust profiles in the descent phase, and so that prescribed speed and altitude constraints at various descent points are satisfied.

Summary of Invention Paragraph:
[0045] According to another aspect of the invention, the weather incident prediction function of the invention communicates with the on-board flight

management system to access the aircraft's intended flight path stored therein and compare it to predicted future position of the storm cell. If the predicted storm cell path and the aircraft's intended flight path coincide, and if conditions, such as phase of flight and storm cell intensity, could threaten the safety of flight, an appropriate warning is issued. Preferably, the warning is issued sufficiently in advance of the predicted coincidence that ample opportunity is afforded for an appropriate course modification.

Detail Description Paragraph:
[0061] The present invention is a method and device for predicting the future path and state, i.e., position and intensity, of a weather condition; comparing the prediction with an aircraft's flight path and other aircraft conditions; and generating a warning if a coincidence will occur and result in a threat to the safety of flight. The warning is any of a visual or aural warning, or both. Historical data and the ability to record and predict the position of a severe weather condition provide the ability to generate a warning five or more minutes before the position of coincidence is encountered. Thus affording ample opportunity for an appropriate course modification. According to one embodiment of the invention, the information describing the future position and intensity of weather conditions is an option available on request, for example, during times of severe weather conditions and/or critical phases of flight.

Detail Description Paragraph:
[0062] FIG. 7 illustrates the weather incident prediction method of the invention for tracking weather condition position and intensity data for a limited time and projecting future path and state data. In FIG. 7, both of a weather radar image data bank 102, and preferably a FMS 104, are coupled to a weather incident prediction function 106, which is coupled in turn to either or both of a visual warning device 108 and an aural warning device 110. A warning is generated if the forecast weather condition track and the aircraft flight path are likely to coincide, and if weather and flight conditions might threaten the safety of flight.

CLAIMS:

20. A method for using an electronic circuit to predict the future position and intensity of a weather condition relative to an aircraft using a weather radar resident on-board the aircraft, the method comprising: recording a first weather radar image generated by an onboard weather radar; recording a second weather radar image generated at a time after said first weather radar image; accessing said first and second recorded weather radar images; with the electronic circuit, referencing said first and second recorded weather radar images to a common physical location; with the electronic circuit, analyzing said first and second weather radar images; with the electronic circuit, predicting a future track of one or more weather cells as a function of said analyzing said first and second weather radar images; displaying said predicted future track of one or more of said weather cells; accessing an intended flight path of the aircraft; accessing a phase of flight of the aircraft; with the electronic circuit, predicting a coincidence of said intended flight path and said weather condition; and with the electronic circuit, determining a potential threat to the safety of flight as a function of said coincidence of said intended flight path, said phase of flight, and said weather condition.

Previous Doc Next Doc Go to Doc#

How Airport Security Works

by Jeff Tyson and Ed Grabianowski

Terrorism has been a problem for airlines and air travelers since the 1970s, when hijackings and bombings became the method of choice for subversive, militant organizations around the world. Although security at airports has always been tight, the 9/11 attacks woke many people up to a harsh reality -- it wasn't tight enough.

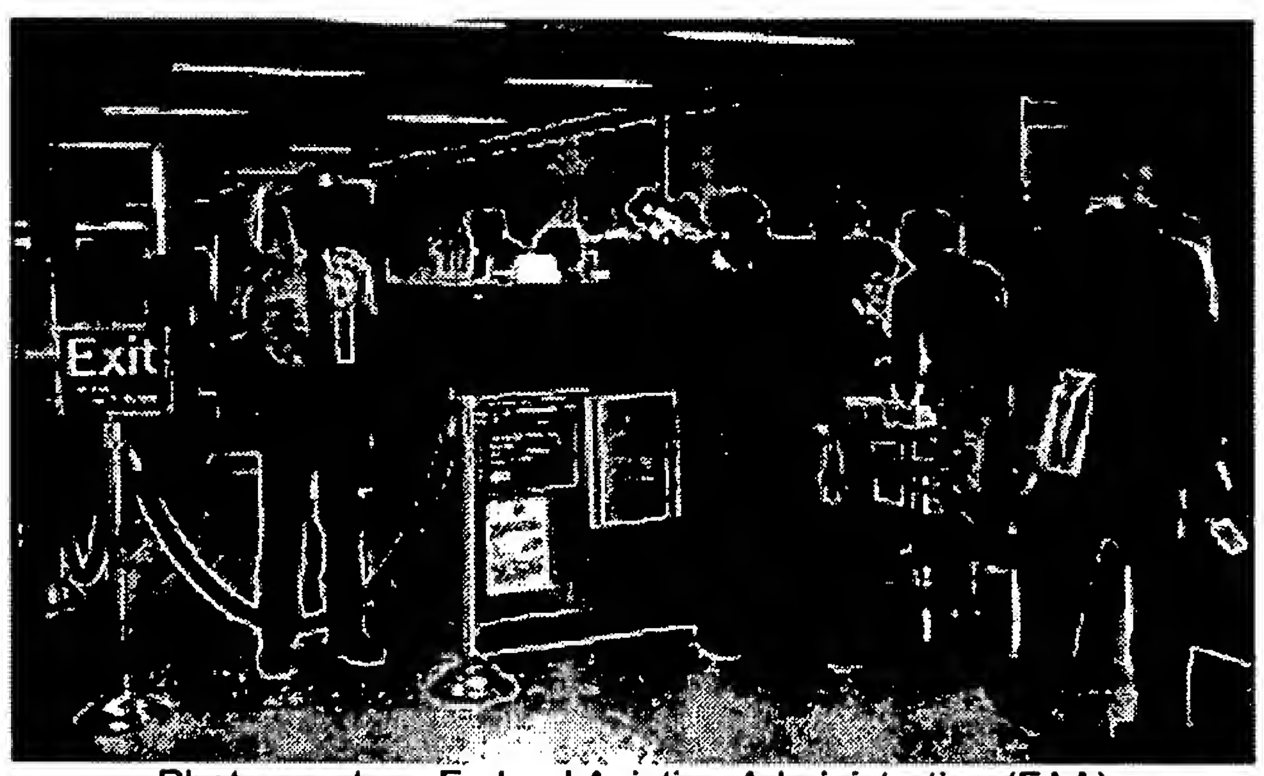


Photo courtesy Federal Aviation Administration (FAA)

Millions of people fly on thousands of planes every day.

On that day, men armed with simple box cutters took over four passenger jets and used them as flying bombs. What security measures might have stopped them? How has airport security changed since then? According to the Department of Homeland Security, 730 million people travel on passenger jets every year, while more than 700 million pieces of their baggage are screened for explosives and other dangerous items. In this article, we'll find out how high-tech solutions are being used to make flying as safe as possible -- and we'll also consider if what we are doing is enough.

Thank You

Special thanks to **Paul Hurd of PerkinElmer Detection Systems** for his assistance with this article.

The First Line of Defense

Imagine for a second that you are a terrorist who wants to blow up or hijack a plane. You know that once you get inside the airport, you will have to pass through metal detectors, bomb-sniffing dogs,

and possibly a search of your clothes and luggage. How could you bypass all of those security measures? You could climb a fence or drive a truck to a sensitive area of the airport.

For this reason, the first line of defense in airport security is the most obvious: fences, barriers and walls. Tall fences that would be difficult to climb enclose the entire airport property. Security patrols regularly scan the perimeter in case someone tries to cut through the fence. Especially sensitive areas, like fuel depots or the terminals and baggage handling facilities are even more secure, with more fences and security checkpoints. All access gates are monitored by either a guard station or surveillance cameras.

Another risk is that someone could drive a truck or car containing a bomb up to the airport terminal entrance and just blow up the airport itself. Airports have taken several steps to prevent this. Large concrete barriers, designed to block vehicles up to the size of large moving trucks, can be deployed if a threat is detected. Loading zones, where people once parked their cars to get their baggage in or out of the trunk, are now kept clear of traffic. No one is allowed to park close to the terminal.

Who Are You?

One of the most important security measures at an airport is confirming the identity of travelers. This is done by checking a photo ID, such as a driver's license. If you are traveling internationally, you need to present your passport.

The photo-identification page of a U.S. passport

Simply taking a look at a photo ID isn't enough, however. The high-tech buzzword in airport security today is **biometrics**. Biometrics essentially means checking fingerprints, retinal scans, and facial patterns using complex computer systems to determine if someone is who they say they are - or if they match a list of people the government has determined might be potential terrorists.

A new system called **CAPPS II** could help accomplish some of this. Short for **Computer Assisted Passenger Prescreening System**, CAPPS II will require more personal information from travelers when they book their flights, which will lead to a risk assessment of no risk, unknown risk, elevated risk, or high risk. Passengers considered risky will be further screened. Although the system has been delayed and isn't in place yet, the Department of Homeland Security (DHS) predicts that CAPPS II will make check-in faster for the average traveler.

You may have noticed the public address system at an airport replaying an automated message telling you not to leave your bags unattended. And you've probably noticed that check-in attendants are asking some questions that sound a little odd:

- Has your luggage been in your possession at all times?
- Has anyone given you anything or asked you to carry on or check any items for them?

These are very important questions. A tactic used on occasion by terrorists is to hide a bomb inside an unsuspecting person's luggage. Another tactic is to give something, maybe a toy or stuffed animal, to someone who is about to board a plane. That innocent-seeming object may actually be a bomb or other harmful device.

Just a month after the 9/11 attacks, the President signed a new law that restructured and refocused the airport security efforts of the U.S. The Aviation and Transportation Security Act established a new agency, the **Transportation Security Administration** (TSA). The TSA is part of the Department of Homeland Security. The TSA's mission is to:

- Prevent attacks on airports or aircraft
- Prevent accidents and fatalities due to transport of hazardous materials
- Ensure safety and security of passengers

While the TSA deals with all forms of transportation, the Federal Aviation Administration (FAA) is devoted entirely to the operation of the U.S.'s civil aviation. FAA agents are located at every major airport for immediate response to possible threats. Most major airports also have an entire police force, just like a small town, monitoring all facets of the facility. Background checks are required on all airport personnel, from baggage handlers to security-team members, before they can be employed. All airport personnel have photo-ID cards with their name, position and access privileges clearly labeled.

Step Through, Please: Metal Detector

All public access to an airport is channeled through the terminal, where every person must walk through a metal detector and all items must go through an X-ray machine.

Almost all airport metal detectors are based on **pulse induction** (PI). Typical PI systems use a coil of wire on one side of the arch as the transmitter and receiver. This technology sends powerful, short bursts (pulses) of current through the coil of wire. Each pulse generates a brief magnetic field. When the pulse ends, the magnetic field reverses polarity and collapses very suddenly, resulting in a sharp electrical spike. This spike lasts a few microseconds (millionths of a second) and causes another current to run through the coil. This subsequent current is called the **reflected pulse** and lasts only about 30 microseconds. Another pulse is then sent and the process repeats. A typical PI-based metal detector sends about 100 pulses per second, but the number can vary greatly based on the manufacturer and model, ranging from about 25 pulses per second to over 1,000.

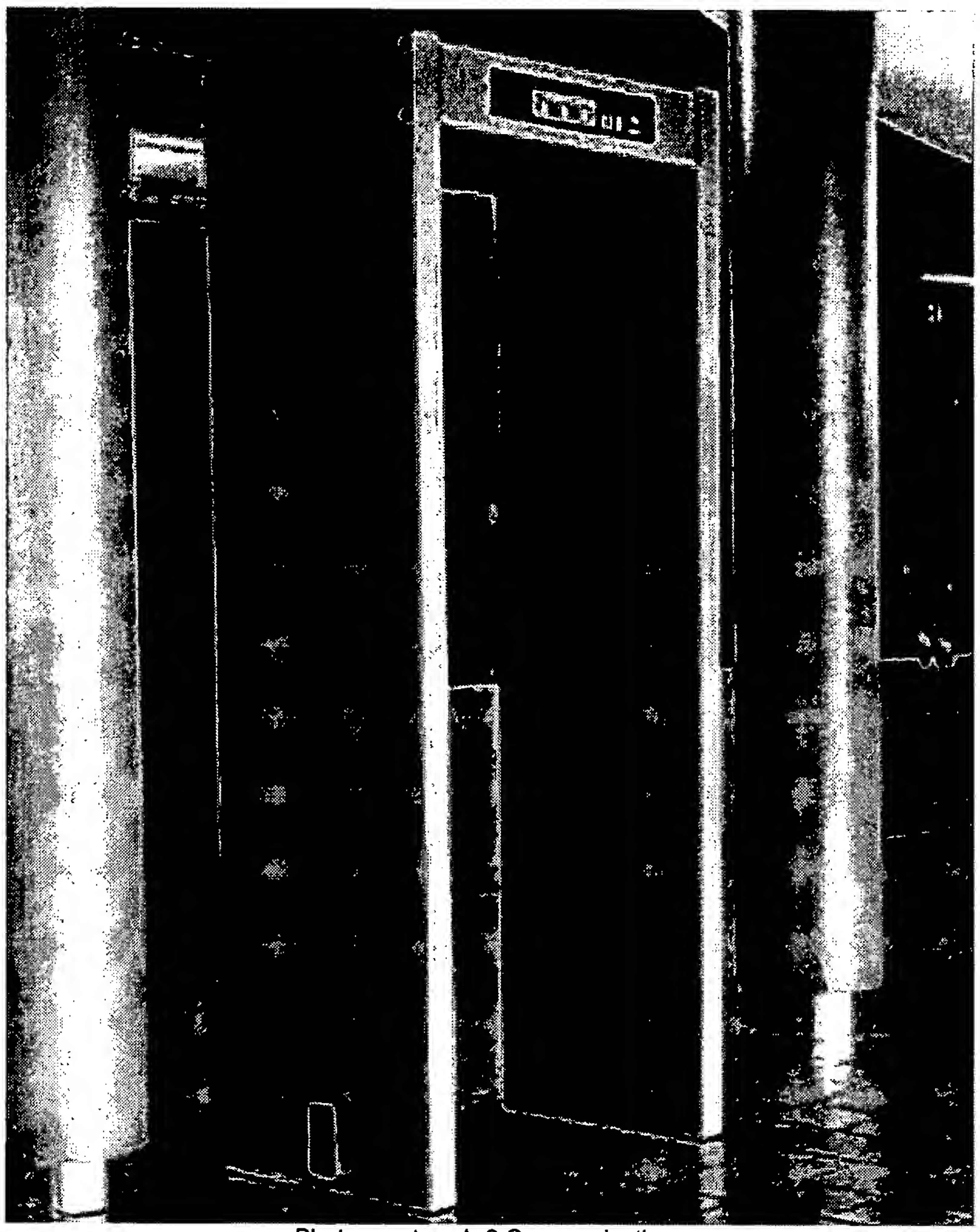
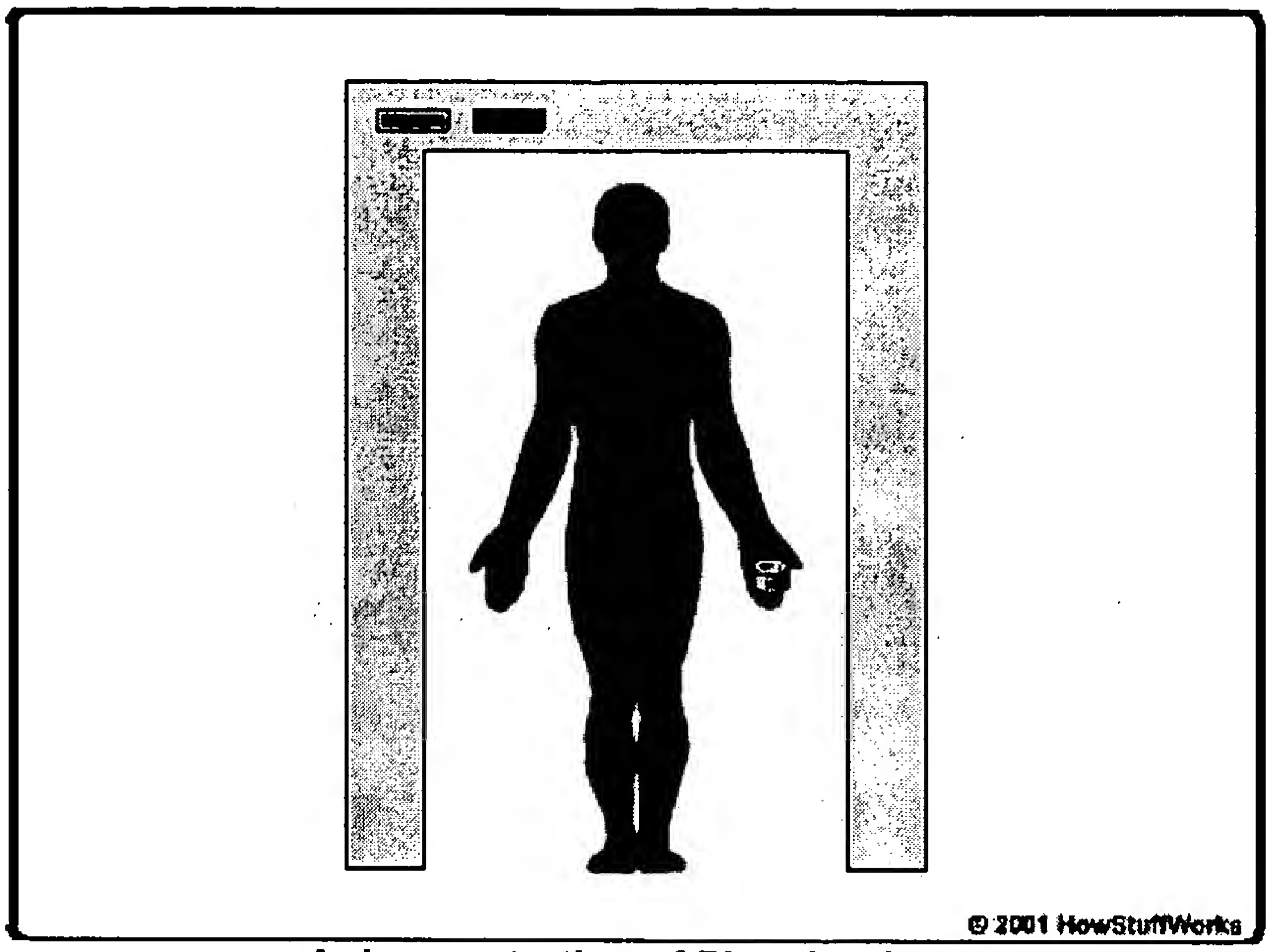


Photo courtesy L-3 Communications
Airport metal detectors rely on pulse induction.

If a metal object passes through the metal detector, the pulse creates an opposite magnetic field in the object. When the pulse's magnetic field collapses, causing the reflected pulse, the magnetic field of the object makes it take longer for the reflected pulse to completely disappear. This process works something like echoes: If you yell in a room with only a few hard surfaces, you probably hear only a very brief echo, or you may not hear one at all. But if you yell into a room with a lot of hard surfaces, the echo lasts longer. In a PI metal detector, the magnetic fields from target objects add their "echo" to the reflected pulse, making it last a fraction longer than it would without them.

A **sampling circuit** in the metal detector is set to monitor the length of the reflected pulse. By comparing it to the expected length, the circuit can determine if another magnetic field has caused the reflected pulse to take longer to decay. If the decay of the reflected pulse takes more than a few microseconds longer than normal, there is probably a metal object interfering with it.



A demonstration of PI technology

The sampling circuit sends the tiny, weak signals that it monitors to a device call an **integrator**. The integrator reads the signals from the sampling circuit, amplifying and converting them to direct current (DC).The DC's voltage is connected to an audio circuit, where it is changed into a tone that the metal detector uses to indicate that a target object has been found. If an item is found, you are asked to remove any metal objects from your person and step through again. If the metal detector continues to indicate the presence of metal, the attendant uses a handheld detector, based on the same PI technology, to isolate the cause.

Many of the newer metal detectors on the market are **multi-zone**. This means that they have multiple transmit and receive coils, each one at a different height. Basically, it's like having several metal detectors in a single unit.

In the next section, we'll discuss what happens to your carry-on items while you're going through the metal detector.

Step Through, Please: X-Ray System

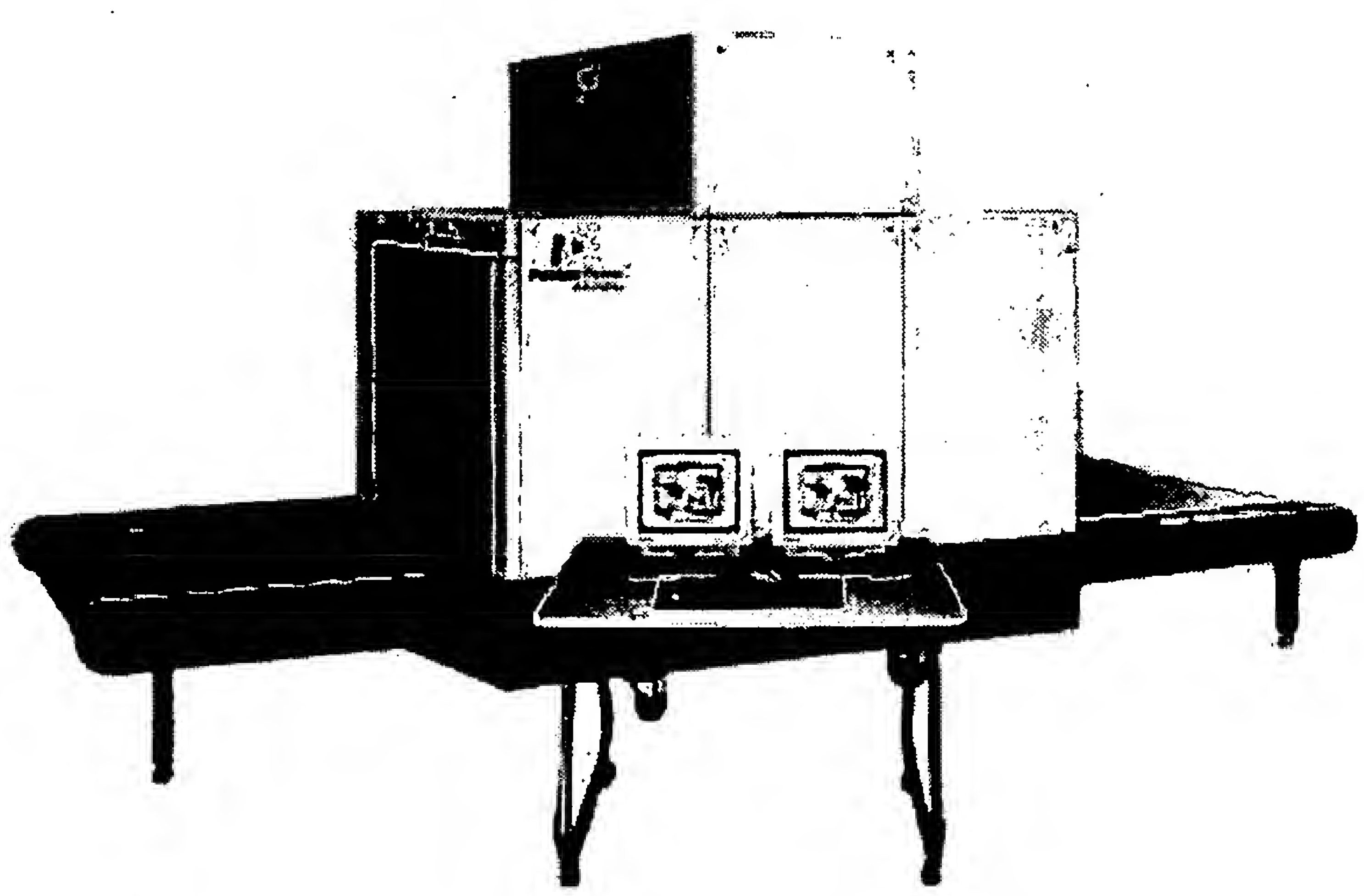


Photo courtesy L-3 Communications
Your carry-on items are sent through a machine that X-rays the contents.

While you are stepping through the metal detector, your carry-on items are going through the X-ray system. A conveyor belt carries each item past an X-ray machine. X-rays are like light in that they are electromagnetic waves, but they are more energetic, so they can penetrate many materials. The machine used in airports usually is based on a **dual-energy X-ray system**. This system has a single X-ray source sending out X-rays, typically in the range of 140 to 160 **kilovolt peak** (KVP). KVP refers to the amount of penetration an X-ray makes. The higher the KVP, the further the X-ray penetrates.

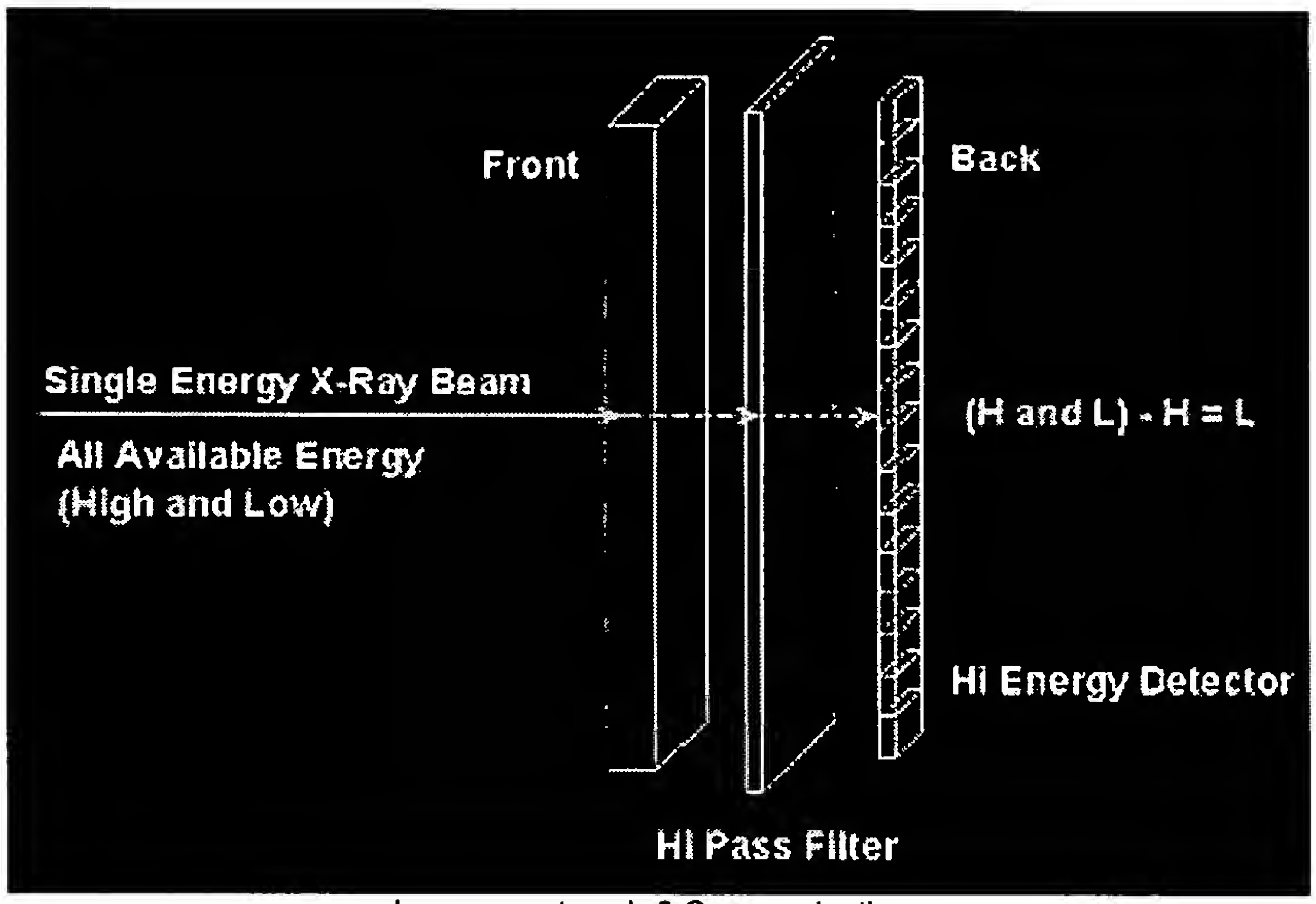


Image courtesy L-3 Communications
In a dual-energy X-ray system, the X-rays pass through a detector, a filter and then another detector.

After the X-rays pass through the item, they are picked up by a **detector**. This detector then passes the X-rays on to a **filter**, which blocks out the lower-energy X-rays. The remaining high-energy X-rays hit a **second detector**. A computer circuit compares the pick-ups of the two detectors to better represent low-energy objects, such as most organic materials.

Since different materials absorb X-rays at different levels, the image on the monitor lets the machine operator see distinct items inside your bag. Items are typically colored on the display monitor, based on the range of energy that passes through the object, to represent one of three main categories:

- Organic
- Inorganic
- Metal

While the colors used to signify "inorganic" and "metal" may vary between manufacturers, all X-ray systems use shades of orange to represent "organic." This is because most explosives are organic. Machine operators are trained to look for suspicious items -- and not just obviously suspicious items like guns or knives, but also anything that could be a component of an **improvised explosive device** (IED). Since there is no such thing as a commercially available bomb, IEDs are the way most terrorists and hijackers gain control. An IED can be made in an astounding variety of ways, from basic pipe bombs to sophisticated, electronically-controlled component bombs.

Photo courtesy L-3 Communications
An X-ray of a bag
Notice that all organic items are a shade of orange.

A common misconception is that the X-ray machine used to check carry-on items will damage film and electronic media. In actuality, all modern carry-on X-ray systems are considered **film-safe**. This means that the amount of X-ray radiation is not high enough to damage photographic film. Since electronic media can withstand much more radiation than film can, it is also safe from damage. However, the CT scanner and many of the high-energy X-ray systems used to examine checked baggage can damage film (electronic media is still safe), so you should always carry film with you on the plane.

Electronic items, such as laptop computers, have so many different items packed into a relatively small area that it can be difficult to determine if a bomb is hidden within the device. That's why you may be asked to turn your laptop or PDA on. But even this is not sufficient evidence since a skilled criminal could hide a bomb within a working electronic device. For that reason, many airports also have a **chemical sniffer**. This is essentially an automated chemistry lab in a box. At random intervals, or if there is reason to suspect the electronic device that someone is carrying, the security attendant quickly swipes a cloth over the device and places the cloth on the sniffer. The sniffer analyzes the cloth for any trace residue of the types of chemicals used to make bombs. If there is any residue, the sniffer warns the security attendant of a potential bomb. In addition to desktop sniffers like this, there are handheld versions, that can be used to "sniff" lockers and other enclosed spaces and unattended luggage. Walk-through models, such as GE's Entry Scan 3, are also available. These sniffers can be used to detect explosives and narcotics.

Now that you have passed through security and are waiting to board your plane, let's see what is happening with your checked baggage.

Check Your Bags: X-ray Systems

In addition to passenger baggage, most planes carry enormous amounts of cargo. All of this cargo has to be checked before it is loaded.

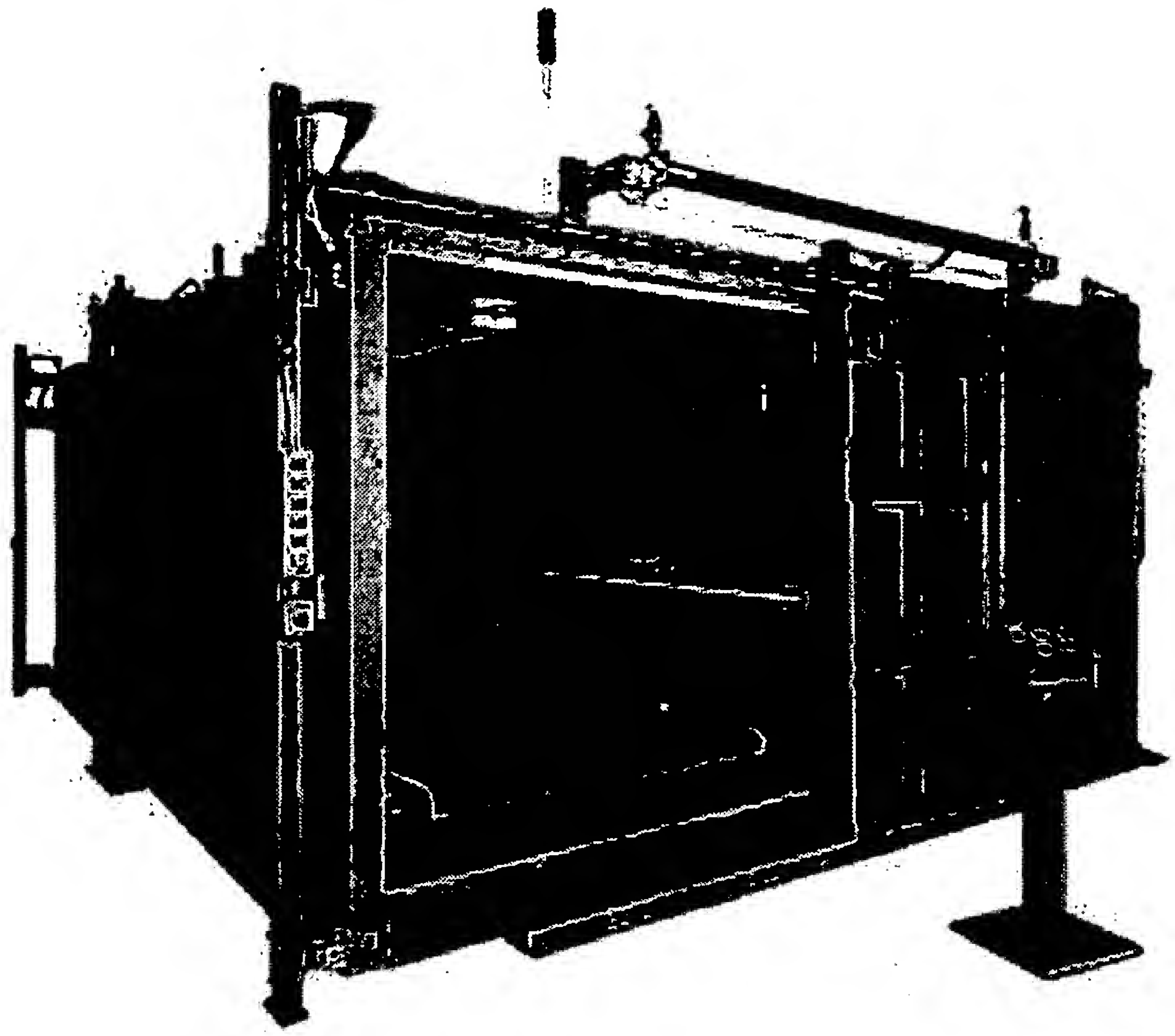


Photo courtesy L-3 Communications
Your luggage goes through a larger X-ray system.

Most airports use one of three systems to do this:

- Medium X-ray systems - These are fixed systems that can scan an entire pallet of cargo for suspicious items.
- Mobile X-ray systems - A large truck carries a complete X-ray scanning system. The truck drives very slowly beside another, stopped truck to scan the entire contents of that truck for suspicious items.
- Fixed-site systems - This is an entire building that is basically one huge X-ray scanner. A tractor-trailer is pulled into the building and the entire truck is scanned at one time.

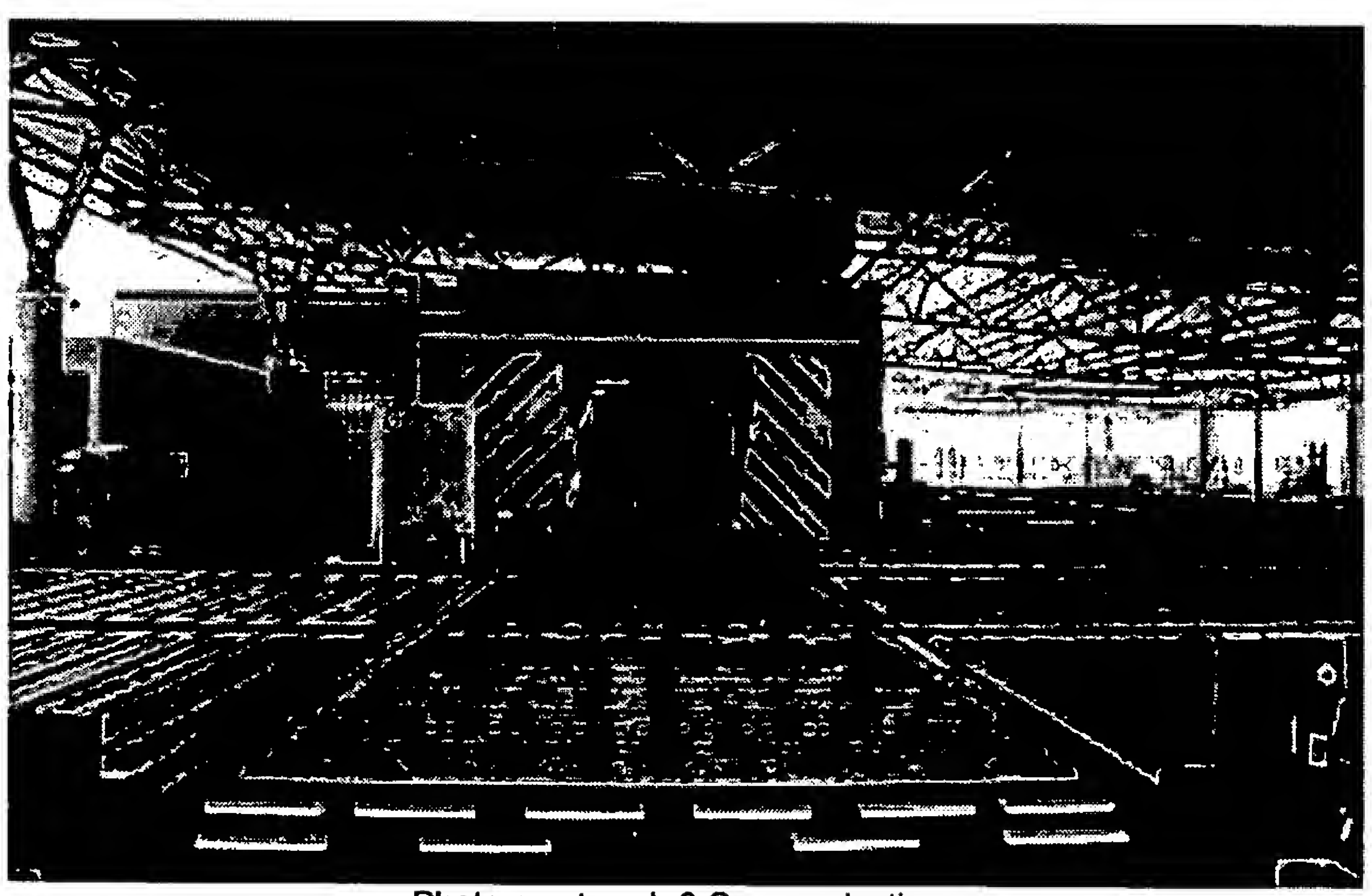


Photo courtesy L-3 Communications
In some airports, medium X-ray facilities are set up to scan an entire pallet of luggage at a time.

One old-fashioned method of bomb detection still works as

well or better than most hi-tech systems -- the use of trained dogs. These special dogs, called **K-9 units**, have been trained to sniff out the specific odors emitted by chemicals that are used to make bombs, as well the odors of other items such as drugs. Incredibly fast and accurate, a K-9 barks at a suspicious bag or package, alerting the human companion that this item needs to be investigated.

Photo courtesy FAA
Dogs are used to sniff for bombs.

In addition to an X-ray system, many airports also use larger scanners. Let's take a look at those next.

Check Your Bags: CT Scanners

The first security check that your checked bags go through depends on the airport. In the United States, most major airports have a **computer tomography (CT) scanner**. A CT scanner is a hollow tube that surrounds your bag. The X-ray mechanism revolves slowly around it, bombarding it with X-rays and recording the resulting data. The CT scanner uses all of this data to create a very detailed **tomogram** (slice) of the bag. The scanner is able to calculate the mass and density of individual objects in your bag based on this tomogram. If an object's mass/density falls within the range of a dangerous material, the CT scanner warns the operator of a potential hazardous object.

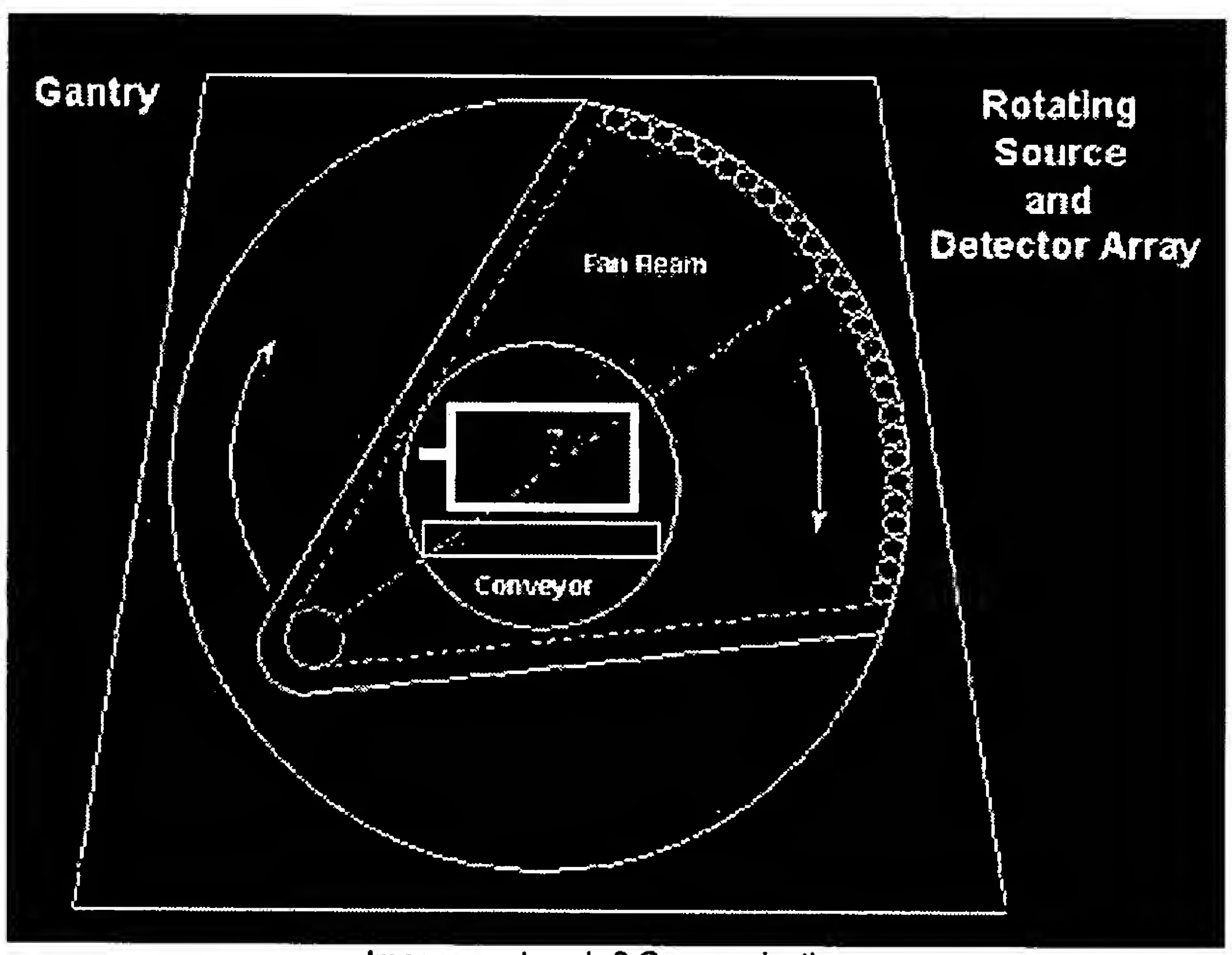


Image courtesy L-3 Communications
This diagram shows how the X-ray system in a CT scanner rotates around a bag.

CT scanners are slow compared to other types of baggage-scanning systems. Because of this, they are not used to check every bag. Instead, only bags that the computer flags as "suspicious" are checked. These flags are triggered by any anomaly that shows up in the reservation or check-in process. For example, if a person buys a one-way ticket and pays cash, this is considered atypical and could cause the computer to flag that person. When this happens, that person's checked bags are immediately sent through the CT scanner, which is usually located somewhere near the ticketing counter.

In most other countries, particularly in Europe, all baggage is run through a scanning system. These

systems are basically larger versions of the X-ray system used for carry-on items. The main differences are that they are high-speed, automated machines integrated into the normal baggage-handling system and the KVP range of the X-rays is higher.

With all of these detectors, scanners and sniffers, it's pretty obvious that you're not allowed take a gun or bomb on a plane. But what else is prohibited?

Now Boarding

While most of the things that you can't take on board an airplane are fairly obvious (guns, knives, explosives), there are some things that most people wouldn't think about. Who would have thought that a smoke detector could be considered hazardous? If you do transport a hazardous material on a passenger plane without declaring it, you could face a fine of up to $27,500! Make sure you contact the local airport authority if you have any concerns about an item you plan to carry with you on a trip.

Because terrorism is a constant and terrifying threat, this means that *any* mention of certain words, such as "bomb," "hijack" or "gun," can lead to your immediate removal from the plane and quite possibly your arrest, even if the word is said in an innocent manner. Everyone who works in aviation, from flight attendants to security personnel, is trained to react immediately to those words.

You Can't Take it With You

There are a number of items that you cannot carry on a plane, and some of that can't be packed in your bags, either:

- **Explosives:** Fireworks, ammunition, sparklers, matches, gunpowder, signal flares
- **Weapons:** Guns, swords, pepper spray, mace, martial arts weapons, swords, knives with blades of any length
- **Pressurized containers:** Hair spray, oxygen tanks, propane tanks, spray paint, insect repellant
- **Household items:** Flammable liquids, solvents, bleach, pool chemicals, flammable perfume in bottles 16 ounces or larger
- **Poisons:** Insecticides, pesticides, rat poison, arsenic, cyanide
- **Corrosives:** Car batteries, acids, lye, drain cleaner, mercury

Air Marshals

If fences and barriers are the first line of defense, the air marshals are the last. If everything else fails and a terrorist still gets onto a flight with a weapon, an armed air marshal can take control of a situation and restrain the attackers. Although the air marshal program has existed since the 1970s, it has never had as high of a profile as it has in the post-9/11 era.

An air marshal is a federal agent disguised to look like regular passenger. Each air marshal is authorized to carry a gun and make arrests. There are not enough air marshals to cover every flight, so their assignments are kept secret. No one knows which passenger is the air marshal, or even if an air marshal is present on the flight at all. Although their exact numbers are kept classified, airline insiders estimate that only five percent of U.S. flights have an air marshal on board. This is still a major increase - in the years before 9/11, a handful of marshals guarded just a few international flights.

In addition to policing the sky, new laws have forced the installation of locks on cockpit doors. This could prevent hijackings by terrorists who are trained to fly passenger jets by keeping them away from

the plane's controls.

Are we doing enough?

While billions of tax dollars are spent beefing up airport security, there are fears that things are still not safe enough. A March 2004 report by the Government Accountability Office (GAO, formerly the General Accounting Office) said that there were still problems "hiring, deploying, and training [TSA's] screener workforce. Staffing shortages and TSA's hiring process continue to hinder its ability to fully staff screening checkpoints."

The GAO also noted the extensive delays in the implementation of CAPPS II, which is far behind schedule and doesn't even have date of completion or cost estimates. The GAO report states, "TSA has not fully addressed seven of eight issues identified by Congress as key elements related to the development, operation, and public acceptance of CAPPS II."

The air marshal program also came under fire in the GAO report - the need for many additional marshals resulted in an abbreviated training program, and budget cuts have further crippled the program. A recent investigation by the DHS's inspector general found 753 reports of air marshal misconduct during an eight-month period in 2002, including sleeping and being drunk while on duty.

Finally, many security experts fear there are too many threats that aren't being addressed at all. Many baggage handlers, mechanics and other technicians with access to airplanes are not screened or searched. Handheld surface-to-air rocket launchers are another concern - currently, U.S. aviation has virtually no defense against such an attack.

For more information on airport security and related topics, check out the links on the next page.

Lots More Information

Related HowStuffWorks Articles

- How Airports Work
- How the Federal Aviation Administration Works
- How Air Traffic Control Works
- How Black Boxes Work
- How Baggage Handling Works
- How Airlines Work
- How Becoming An Airline Pilot Works
- How Airline Crews Work
- How Customs Works
- How Airline Freight Works
- How Airplanes Work
- How Helicopters Work
- How Metal Detectors Work
- How Police Dogs Work
- How X-rays Work
- I've noticed that I am not allowed to use my cell phone in airplanes or in hospitals. Why are these prohibitions in place?
- How does an EPIRB distress radio work?

More Great Links

- PerkinElmer Detection Systems
- GE Explosives and Narcotics Detection
- FAA Homepage
- AirSafe.com
- Office of Aviation Research

Sources

- Air marshals cover only a few flights.August 16, 2004 Airport security - a work in progress. Feb. 23, 2004
- Government Accountability Office (2004). Improvements Still Needed in Federal Aviation Security Efforts. GAO-04-592T

Refine Search

Your wildcard search against 10000 terms has yielded the results below.

Your result set for the last L# is incomplete.

The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

Search Results -

Terms	Documents
L11 and ((chang$ or correct$ or modif$) with differen$ with (path$ or route or way$ or course))	0

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L14

Refine Search

Recall Text Clear Interrupt

Search History

DATE: Friday, November 25, 2005 Printable Copy Create Case

Set Name side by side	**Query**	**Hit Count**	**Set Name** result set
	DB=PGPB,USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L14	L11 and ((chang$ or correct$ or modif$) with differen$ with (path$ or route or way$ or course))	0	L14
L13	L11 and biometr$	2	L13
L12	L11 and ((secur$ or saft$) with (path$ or way$ or route))	2	L12
L11	l9 or L10	4	L11
	DB=PGPB; THES=ASSIGNEE; PLUR=YES; OP=OR		
L10	20050001711	1	L10
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L9	6810310.pn. or 6691956.pn. or 5067674.pn.	3	L9

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR

L8	L7 and biometr$	4	L8
L7	L6 or L1	680	L7
L6	(safe$ with (flight$ with path$)) and @pd<=20040426	344	L6
L5	L3 not L4	16	L5
L4	L3 and security	2	L4
L3	L2 and (701/3).ccls.	18	L3
L2	(safe$ with (flight$ with path$)) and @ad<=20040426	284	L2
L1	(safe$ same (flight$ with path$)) and @ad<=20040426	567	L1

END OF SEARCH HISTORY

PALM Intranet

Application Number [ ] SEARCH

IDS Flag Clearance for Application 10709268

IDS Information

Content	Mailroom Date	Entry Number	IDS Review	Reviewer
M844	02-22-2005	24	☑	03-09-2005 09:24:41 rbaltimore

UPDATE

Refine Search

Your wildcard search against 10000 terms has yielded the results below.

Your result set for the last L# is incomplete.

The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

Search Results -

Terms	Documents
L11 and ((chang$ or correct$ or modif$) with differen$ with (path$ or route or way$ or course))	0

Database:

US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L14

Refine Search

Recall Text Clear Interrupt

Search History

DATE: Friday, November 25, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L14	L11 and ((chang$ or correct$ or modif$) with differen$ with (path$ or route or way$ or course))	0	L14
L13	L11 and biometr$	2	L13
L12	L11 and ((secur$ or saft$) with (path$ or way$ or route))	2	L12
L11	l9 or L10	4	L11
	DB=PGPB; THES=ASSIGNEE; PLUR=YES; OP=OR		
L10	20050001711	1	L10
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L9	6810310.pn. or 6691956.pn. or 5067674.pn.	3	L9

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR

L8	L7 and biometr$	4	L8
L7	L6 or L1	680	L7
L6	(safe$ with (flight$ with path$)) and @pd<=20040426	344	L6
L5	L3 not L4	16	L5
L4	L3 and security	2	L4
L3	L2 and (701/3).ccls.	18	L3
L2	(safe$ with (flight$ with path$)) and @ad<=20040426	284	L2
L1	(safe$ same (flight$ with path$)) and @ad<=20040426	567	L1

END OF SEARCH HISTORY

Y +

L21: Entry 3 of 13 File: PGPB Mar 25, 2004

DOCUMENT-IDENTIFIER: US 20040056770 A1
TITLE: Hijack disabling system for commercial aircraft and other vehicles

Pre-Grant Publication Date:
20040325

Application Filing Date:
20020919

Summary of Invention Paragraph:
[0014] In a similar manner, the AFCS of the present invention disincentivizes would-be hijackers and/or terrorists from aircraft hijackings, by implementing an aircraft security system that securely engages an aircraft's automated flight control system and irreversibly overrides onboard control of aircraft at any point that a hijacking is suspected, or attempted. Thus, by terminating the onboard control of the plane, the system prevents aircraft laden with thousands of gallons of jet fuel from being commandeered as high-speed `guided missiles`. The system also precludes any resetting of a hijacked aircraft's AFCS system until one or more authorized personnel located at an arrival-airport boards the landed aircraft and manually resets the system. Thus, the landed aircraft is incapacitated until its system is manually reset.

Summary of Invention Paragraph:
[0021] New commercial aircraft are already equipped with computer-controllable flight systems, capable not only of following a predetermined (or programmable) flight path, but of safely landing such aircraft at commercial airports. The present invention provides a method for:

Detail Description Paragraph:
[0048] The vehicle's computer(s) are preferably equipped to handle the reception of signals sent from a plurality of transmitters simultaneously and the computer(s) and software running thereon is responsive to the signals to change the automated mode of the computer(s). The vehicle computer(s) can also be equipped with at least one software routine that prevents any change in the operation of the computer(s) by anyone aboard an operating vehicle, once the computer(s) has been set to the automated mode, in which case, the computer(s) can be programmed so that it can only be reset by at least one authorized security person who boards the vehicle after any threat to a vehicle or to persons aboard a vehicle has been eliminated and the vehicle is deemed safe and secure by authorized security personnel. The vehicle, or onboard, computer(s) are preferably programmed to have at least one `false deployment` software routine that provides for a resetting of the computer (s) from the automated mode to an non-automated mode when, as a result of consultation between one or more flight crew member and one or more flight personnel and/or flight marshal, the flight crew is convinced that a emergency signal was either, sent by mistake, or a threat to the vehicle, has been eliminated. The software of the computer(s) can also be programmed so that `false deployment` software routine(s) can only be executed within a predetermined limited time period following a setting of the computer(s) to the automated mode, for example within a pre-determined limited time period of less than 10 minutes after the computer(s) is set to the automated mode. Additionally, the computer(s)

software can be programmed so that the `false deployment` software routine(s) can only be executed after the computer(s) is set to the automated mode and following the reception of subsequent secure electronic signal sent from a plurality of transmitters operated by vehicle-personnel aboard the vehicle. For example, an in-flight procedure can require that one or more, or all, flight personnel assemble after a false deployment, or after an eliminated in-flight threat, to, on a verbal cue, all transmit a post-deployment signal to the computer(s) which resets the computer(s) to a non-automated mode when the signals are received within the pre-determined limited time period (e.g. less than 10 seconds.) As an added precaution, the aircraft can thereafter be closely monitored by one or more independent facility, such that, if there is any diverting of the aircraft exceeding a predetermined time period and no communications from the aircraft regarding such diversion is made, or it is apparent that the aircraft is headed toward a desireable terrorist target, the system will automatically revert to the former automated mode or accept a signal from one or more of the facilities to place the computer into an automated mode. Many aircraft, such as those used in the 9/11 attacks, have a FMC and/or FMS and have fly-by-wire flight controls capable of disabling human/manual input from within the cockpit, the system of the present invention overrides cockpit flight control when the aircraft is in an automated mode.

Detail Description Paragraph:
[0053] Each secure, independent facility(s) is equipped to grant "top priority status" to a moving vehicle under automated computer control, to clear all other like vehicles out of its way on any route the vehicle takes and to any destination it goes to, and the facility is also equipped with communications means to contact any transportation-related and security entity necessary to notify them of the vehicle's status and the type of threat the vehicle poses. Vehicle computer(s) are optionally equipped to be programmed to automatically set a vehicle into an automated mode if the vehicle is diverted from a expected path for longer than a predetermined threshold time period and when no communication from the vehicle has been made during the alloted time period. For example, if an aircraft is diverted significantlly off course, or is significantly changing its altitude, for more than a preset number of minutes and no communication from the aircraft flight crew explaining its actions is received, the computer(s) can set the aircraft in an automated flight mode and disable in-cockpit human flight control. Similarly, if the vehicle is not sending transponder signal for longer than a predetermined threshold time period and when no communication from the vehicle has been made during the time period the computer(s) can set the aircraft in an automated flight mode and disable in-cockpit human flight control.

Detail Description Paragraph:
[0054] In the event that a vehicle, such as a commercial aircraft is guided in an automated mode to a pre-determined destination, and a hostile or threatening condition still exists aboard the aircraft, an embodiment of the hijack disabling system provides for equipping aircraft with at least one orifice and coupling means for coupling one end of a gas conduit thereto, and providing a supply of at least one incapacitating gas having a gas outlet and coupling means for coupling an opposite end of the gas conduit thereto, and control means for controlling the flow of the gas through the conduit into the vehicle as needed. When needed, the gas is conveyed through the gas conduit into the orafice which in turn, is coupled to least one gas outlet leading to the aircraft cabin. Those aboard the aircraft become incapacitatedd when the volume of the gas relative to the normal volume of air in the cabin reaches a known threshold.

Detail Description Paragraph:
[0055] Optionally, the vehicle computer(s) can be programmed and have a user interface to provide for, the entering of a transportation mode change access code to revert the computer(s) from an automated mode to a non-automated mode when a crew member controlling the vehicle is convinced after conferring with a plurality

of vehicle personnel that a "false deployment" mistakenly sent by at least one vehicle personnel has caused the vehicle to enter an automated mode, or when an onboard threat has been successfully eliminated. The computer(s) can also be programmed to automatically set the vehicle back into an automated mode after an access code is entered, if the vehicle is diverted from a expected path for longer than a predetermined threshold time period and when no communication from the vehicle has been made during the time period.

CLAIMS:

56. The system of claim 1 wherein said vehicle is an aircraft and each of said at least one path is a flight vector programmable in and executable by said computer (s) and at least one of said vectors(s) ends on a runway of an airport and said at least one automated mode is an automated safe landing of said aircraft.

62. The system of claim 1 further comprising said computer(s) being programmed to automatically set a vehicle into an automated mode if said vehicle is diverted from a expected path for longer than a predetermined threshold time period and when no communication from the vehicle has been made during said time period.

63. The system of claim 1 further comprising said computer(s) being programmed to automatically set a vehicle into an automated mode if said vehicle is not sending transponder signal for longer than a predetermined threshold time period and when no communication from the vehicle has been made during said time period.

66. The system of claim 1 further comprising: said computer(s) being programmed to, and having a user interface to provide for, the entering of a transportation mode change access code to revert said computer(s) from an automated mode to a non-automated mode when a crew member controlling the vehicle is convinced that a "false deployment" mistakenly sent by at least one vehicle personnel has caused the vehicle to enter an automated mode, and said system further comprising said computer(s) being programmed to automatically set said vehicle back into an automated mode if said vehicle is diverted from a expected path for longer than a predetermined threshold time period and when no communication from the vehicle has been made during said time period.

Previous Doc   Next Doc   Go to Doc#

informs

INFORMS homepage

Editor-in-Chief OR Homepage

INFORMS Publications Information Page

PubsOnLine for Members/Subscribers

INFORMS Conferences

Contact INFORMS Customer Service

Username

Password

Register or login

Athens Login

Forgotten your password?

View my basket

exenza

Browse Search My Profile Activate

Home > List of Issues > Table of Contents > Abstract

Free-Flight and en Route Air Safety: A First-Order Ar

Author(s): Arnold Barnett[1]

doi: 10.1287/opre.48.6.833.12394

View PDF article (149 K)
View table of contents
Add to my alerts
RSS What is RSS?
Trouble viewing articles as PDF?

View references
Email this link

Operations Research

Print ISSN: 0030-364X | **Electronic ISSN:** 1526-5463 | **CODEN:** OPREAI
Volume: 48 | **Issue:** 6
Cover date: Nov. - Dec. 2000
Page(s): 833-845

Keywords

Transportation, safety: aviation collision risk modeling, Reliability, failure models: risk

Abstract text

Under present arrangements, U.S. commercial planes do not travel "as the crow to destination; rather, they are generally restricted to paths within a grid. New tec however, raise the possibility of moving to a "free-flight" regime under which plan directly from point to point. Striving for general insight rather than definitive conclu geometrical probability to assess how free-flight could affect the safety and efficie air traffic operations. We work with two air traffic control sectors: one hypothetica based on actual traffic patterns over Albany, New York. Though tentative, the res that—so long as certain operational constraints are retained—the changed geom paths after a transition to free-flight might tend in itself to diminish mid-air collision depends, however, on whether the human/technological capabilities of future air match the extraordinary effectiveness of the existing system.

Author(s) affiliations

1. Sloan School of Management, Operations Research Center, Massachusetts In Technology, Cambridge, Massachusetts 02139
abarnett@mit.edu

NEWS RELEASE

For Immediate Release

Contact Barry List, PR Director, (410) 691-7852; (800) 4INFORMS; (410) 358-7162h; pager (410) 368-6580; barry.list@informs.org

O.R. STUDY SUGGESTS SAFETY BENEFITS FROM FREE FLIGHT ROUTINGS

The Catch: The Geometry Works; Will the Technology?

LINTHICUM, MD, January 31 – Free flight, which would cut travel time by routing air traffic directly between airports, might be just as safe as the current air traffic control system that holds airplanes to grid paths, according to a preliminary study published in a journal of the Institute for Operations Research and the Management Sciences (INFORMS®).

Shortened flight paths could also translate to reduced costs for the nation's airlines.

"The changed geometry of flight paths after a transition to free-flight tends in itself to diminish mid-air collision risk," says Arnold I. Barnett, George Eastman Professor of Management Science, the Sloan School, Massachusetts Institute of Technology.

"But there is an important caveat: Free-flight would also replace the orderly patterns that now appear on an air traffic controller's screen with something closer to the random scatter of gas molecules. Computer aids are supposed to prevent confusion, but their success must be demonstrated before we can be sure that they can preserve the extraordinary safety of the present system."

The study, "Free-Flight and En Route Air Safety: A First-Order Analysis," appears in the current issue of *Operations Research*, an INFORMS publication.

Antiquated Paths

In U.S. airspace, planes generally cannot travel the straight-line paths from their origins to their destinations. Rather, they usually are restricted to a series of fixed routes that are the aerial equivalent of the interstate highway system. The specific paths were selected more than half a century ago, and radar beacons for navigation were placed along them.

Recent advances in technology, however, raise the possibility that present arrangements can be replaced by a "free-flight "regime, under which planes generally could travel directly from one city to another. Among these advances are global positioning satellites, new ground/air communication links, enhanced collision-avoidance systems aboard planes, and powerful automation aids to air-traffic controllers.

The benefits of free-flight include shorter trip time, lesser fuel consumption, and additional flights.

Prof. Barnett applied operations research models to the geometry of flying in and out of a hypothetical square air sector.

"My basic view," he says, "is that the geometric consequences of free-flight — reduced path crossings and lesser angles at which crossings occur — might *in themselves* be expected to increase safety."

His results showed a "safety dividend" as high as 69% under free flight. The geometric safety dividend reflects fewer flight-path crossings under the proposed system, as well as changes in crossing angles which tend to allow more time to avert disaster when two planes are on a collision course. Free flight reduced mean transit distance by 11% in the initial case Prof. Barnett studied.

When the research was repeated with data from a representative air sector above Albany, New York the results were more modest but still significant. In the Albany example, mean transit distance improved by 2%, the limited improvement largely a tribute to the skill with which the original aerial "highways" were chosen to fit demand patterns. The safety dividend based on changed geometry improved by 58%.

The results could mean savings for airliners, says Prof. Barnett. A 2% reduction in average flight paths – barring erosion of this effect in the air terminal areas – would imply a 2% drop in en route fuel consumption and the shortening of typical flights by a few minutes. Given annual fuel costs of about $50 billion for US domestic jet carriers, savings could come to $1 billion a year, roughly one-fifth of the industry's total annual profit in the late 1990s.

The results also imply that free flight might allow air carriers to double the number of flights through an air sector while maintaining current safety figures.

The Albany data analyzed in the study represented traffic on July 22, 1994; it was supplied by the Federal Aviation Administration's Boston center.

Important Caveats

Prof. Barnett cautions that actual savings could be less if congestion around the nation's airports leads to airplanes using additional fuel before landing. He notes that results in a single sector may not generalize to the totality of air sectors around the country because of differences in flight patterns in different sectors.

Prof. Barnett points out that his research involves a number of idealized assumptions.. He assumes free-flight in latitude and longitude but not altitude; thus, planes could not simply announce that they would travel at, say, 37,000 feet but would be required to fly at a mandated altitude. (Prof. Barnett suggests that two-dimensional free flight might be considerably more prudent than a three-dimensional version.)He only examines planes that have achieved a fixed high altitude and are en route, rather than taking off or landing. He also generally assumed that all en-route aircraft cruise at the same speed (though he relaxed that assumption in one exercise).

The Institute for Operations Research and the Management Sciences (INFORMS®) is an international scientific society with over 10,000 members, including Nobel Prize laureates, dedicated to applying scientific methods to help improve decision-making, management, and operations. Members of INFORMS work in business, government, and academia. They are represented in fields as diverse as airlines, health care, law enforcement, the military, the stock market, and telecommunications. The INFORMS website is at http://www.informs.org.

###

Section 1A Technologies for Future Spaceports and Ranges
Autonomous Flight Safety System

Autonomous Flight Safety System (AFSS) is an independent flight safety system designed for small to medium sized expendable launch vehicles launching from or needing range safety protection while overlying relatively remote locations. AFSS replaces the need for a man-in-the-loop to make decisions for flight termination. AFSS could also serve as the prototype for an autonomous manned flight crew escape advisory system.

AFSS utilizes onboard sensors and processors to emulate the human decision-making process using rule-based software logic and can dramatically reduce safety response time during critical launch phases. The Range Safety flight path nominal trajectory, its deviation allowances, limit zones and other flight safety rules are stored in the onboard computers. Position, velocity and attitude data obtained from onboard global positioning system (GPS) and inertial navigation system (INS) sensors are compared with these rules to determine the appropriate action to ensure that people and property are not jeopardized. The final system will be fully redundant and independent with multiple processors, sensors, and deadman switches to prevent inadvertent flight termination.

AFSS is currently in Phase III which includes updated algorithms, integrated GPS/INS sensors, large scale simulation testing and initial aircraft flight testing.

Bob Ferrell (Primary Contact)
NASA YA-D7
Kennedy Space Center, FL 32899
Bob.A.Ferrell@nasa.gov
(321)-867-6678

James Simpson
NASA YA-D7
Kennedy Space Center, FL 32899
James.C.Simpson@nasa.gov
(321) 867-6937

Roger Zoerner
ASRC-10
Kennedy Space Center, FL 32899
Roger.Zoerner-1@ksc.nasa.gov
(321) 861-2960

Barton Bull
NASA GSFC/WFF Code 598
Wallops Island, VA 23337
Barton.Bull@nasa.gov
(757) 824-1893

Jim Lanzi
NASA GSFC/WFF Code 598
Wallops Island, VA 23337
Raymond.J.Lanzi@nasa.gov
(757) 824-2492

First Hit Previous Doc Next Doc Go to Doc#

End of Result Set

Generate Collection Print

L1: Entry 1 of 1 File: PGPB Mar 25, 2004

PGPUB-DOCUMENT-NUMBER: 20040056770
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20040056770 A1

TITLE: Hijack disabling system for commercial aircraft and other vehicles

PUBLICATION-DATE: March 25, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY
Metcalf, Darrell J.	Fillmore	CA	US

APPL-NO: 10/246073 [PALM]
DATE FILED: September 19, 2002

INT-CL: [07] G08 B 13/00

US-CL-PUBLISHED: 340/574; 701/011, 701/002
US-CL-CURRENT: 340/574; 701/11, 701/2

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

A system for preventing the hijacking, or suicide-bombing, of aircraft, ocean-going vessels, or trains, having at least one onboard vehicle computer capable of operating the vehicle in an automated transportational mode along at least one path when any attempt to overtake or divert the vehicle is made or suspected, or threat of harm to any vehicle-personnel is made or suspected. The system has at least one signal receiver interfaced with, and having a communication link with, the computer (s), and the computer(s) is configured to be responsive to at least one secure signal when initiated by at least one user aboard the vehicle and sent from at least one signal transmitter to the signal receiver(s). The transmitter(s) has an easy-to-use user-interface which is operated by an engagement of at least one finger of user's hand to cause the signal to be sent to the receiver(s). The computer(s) have at least one software routine which is enabled when the signal is received by the receiver(s) and which causes the computer to operate the vehicle in at least one automated mode. When in the automated mode, all manual control of the vehicle is disabled and the vehicle is automatically directed to a pre-determined programmable destination. The system accommodates a resetting of the computer(s) to a non-automated mode when there is a false deployment and security checks and balances are provided from a secure, independent facility having the means to communicate with those aboard a vehicle and to transmit control signals to the vehicle's system.

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This is a non-provisional patent application, which relies substantially on provisional patent application No. 60/322,904 filed Sep. 17, 2001.

Previous Doc Next Doc Go to Doc#